Rule 20. County Security Procedures

20.1 The county must submit its security plan on the form prescribed by the Secretary of State in accordance with section 1-5-616(5), C.R.S., not less than 60 days before an election. A county must also submit a comprehensive procedure for ballot delivery in an emergency under section 1-7.5-115(1), C.R.S.

20.2 The county may not install any software on any component of the voting system unless directed to, or approved by, the Secretary of State.

20.3 General requirements concerning security documentation

20.3.1 The county must maintain on file all documentation of seals, chain-of-custody, access logs, trusted build, and other documents related to the transfer of equipment between parties. These documents are subject to inspection by the Secretary of State. All written entries must be completed in permanent ink.

20.3.2 The county must maintain and document uninterrupted chain-of-custody for each voting device from the installation of trusted build to the present, throughout the county's ownership or leasing of the device. For ballot scanners approved for use under section 1-5-613(2), C.R.S. but for which no trusted build exists, the county must maintain and document uninterrupted chain-of-custody for each voting device from the successful completion of acceptance testing conducted according to Rule 20.10.4.

20.3.3 Only election officials or canvass board members sworn under oath are allowed to handle ballots.

20.3.4 Any form or log containing "date" means to note the month, calendar day, year, hour, minute, and whether the time is a.m. or p.m.

20.3.5 The county must submit sample copies of all referenced forms, schedules, logs, and checklists with the security plan.

20.4 Physical locking mechanisms and seals. The county must record the serial number of every seal on the appropriate chain-of-custody log. Two individuals must verify, and indicate by signing and dating the log, that the seal serial numbers match the logged serial numbers. If a seal is inaccessible and cannot be removed, then it is not necessary to verify that seal serial number.

20.4.1 Counties must continuously comply with the seal requirements of the most recent conditions of use issued by the Department of State for the county's voting system. Counties may not allow any unattended voting system component to remain unsealed at any point after trusted build has been installed on the component.

20.4.2 Activation cards

(a) The county must assign and securely affix a permanent unique identifier to each removable card or activation card. The county may use the manufacturer assigned serial number for this purpose.

(b) The county must handle activation cards in a secure manner at all times. The county must transfer and store any card or activation card in a secure container with at least one seal. Upon delivery and receipt, election judges or county personnel must verify, and indicate by signing and dating the chain-of custody log, that all seal numbers match those listed in the log.

(c) The county must maintain a written or electronic log to record activation card seals and track seals for each voting unit.

(d) The county must maintain a complete inventory of activation cards, including which VSPC they are assigned to during an election. Before and after a VSPC opens and closes each day, the supervisor judge must verify that all cards issued to the VSPC are present. If at any time the supervisor judge cannot account for all activation cards issued to the VSPC, the supervisor judge or a member of the county election staff must immediately submit an incident report to the Secretary of State under Rule 11.7.

20.5 Access to secure areas and voting systems

20.5.1 The county must change all keypad door codes or locks and vault combinations to secure areas as outlined in Rule 20.9.3, at least once per calendar year prior to the first election of the year.

20.5.2 The county must state in its security plan the name, title, and date of most recent background check for each employee with access to areas identified in Rule 20.5.3.

20.5.3 The county may grant access to the areas and the codes, locks, or combinations described in this Rule in accordance with the following limitations:

(a) Access to the code, lock, or combination to ballot storage areas, counting room, location of adjudication, or tabulation workstations is restricted to employees who have successfully passed a criminal background check. Any person who has been convicted of an election offense or an offense with an element of fraud is prohibited from having access to the above areas.

(b) Any individual who is prohibited from having physical contact with any voting equipment under section 1-5-607(1), C.R.S. may not access a room with voting equipment unless accompanied by one or more individuals with authorized access.

(c) Except for emergency personnel, no other individuals may be present in these locations unless supervised by one or more employees with authorized access.

(d) In extreme circumstances, the county may request and the Department of State may grant exemption from the requirements outlined in this Rule.

20.5.4 Voting system access security

(a) Except for voters using a voting system component to vote during an election, county clerks may not allow any person to access any component, including the hard drive(s) or copies of any part of the hard drive(s) for any component, of a county's voting system unless that person has passed the background check required by this or any other rule or law, is performing a task permitted by the county clerk or the Department of State under statute or rule, and is:

(1) An employee of the county clerk;

(2) Appointed as an election judge by the county clerk in accordance with Article 6 of Title 1, C.R.S.;

(3) An employee of the voting system provider for the county's voting system; or

(4) An employee or designee of the Department of State.

(b) All voting system provider employees who conduct work on any component of a county's voting system must complete a criminal background check prior to the employee's work with the voting system. The provider must affirm that the check was conducted in writing to the Department of State prior to the employee conducting any work. Any person convicted of an election offense or an offense with an element of fraud is prohibited from working on any component of a county's voting system.

(c) All Department of State staff who conduct work on any component of a county's voting system must undergo a criminal background check prior to the staff's work with the voting system.

(d) Any person convicted of an election offense or an offense with an element of fraud is prohibited from working on any component of a county's voting system.

(e) Any violation of Rule 20 may result in the prohibition or limitation on the use of, as well as decertification of, a county's voting system or components in accordance with section 1-5-621, C.R.S., and Rule 21.7.3.

20.5.5 Access to where election management software is used is limited to authorized election officials and watchers only. Messengers or runners delivering ballots between the preparation room and computer room must wear distinguishing identification.

20.6 Internal Controls for the Voting System

20.6.1 In addition to the access controls discussed in Rule 20.5, the county must change all passwords and limit access to the election management system by doing the following:

(a) The county must change all passwords associated with a voting system according to the schedule required by the most recent conditions of use for that voting system.

(b) Administrative and user accounts for the operating system on the voting system, election management system and election projects.

(1) The county may use the administrative user account for the election management system only to create individual user accounts for each election project.

(2) The county must create individual user accounts that are associated and identified with each individual authorized user of the operating system of the voting system, election management system or election project.

(3) The county must restrict access to each individual user account with a unique password known only to each individual user. Authorized users must access the operating system of the voting system, election management system, and election project using his or her individual user account and unique password.

(4) The county may grant administrative privileges to no more than four individual user accounts per election unless the county has requested and been authorized by the Department of State to grant more. The county must identify the employees with administrative privileges in the security plan filed with the Department of State.

(5) The county may only grant administrative privileges for the operating system of the voting system to the county clerk, employees of the county, and any person appointed by the Department of State to assist in the administration of an election, subject to the restrictions of Rule 20.6.1 (b)(8). The county may only grant administrative privileges to the election management system or the election project to the county clerk, employees of the county clerk's office, and any person appointed by the Department of State to assist in the administration of an election, subject to the restrictions of Rule 20.6.1 (b)(8).

(6) Authorized users with administrative privileges of the operating system, election management system, or election project may not share their accounts or passwords with anyone.

(7) The county must disable all accounts to access the operating system for individuals who are no longer employed by the county, or are no longer employed in a role that requires access to the voting system.

(8) Any individual who is prohibited from having physical contact with any voting equipment under Section 1-5-607 (1), C.R.S. may not grant themselves or be granted with an account or password for the operating system of the voting system, the election management system, or an election project.

(c) The voting system provider may not have administrative or user access to the county's election management system.

(d) The county may not connect or allow a connection of any voting system component to the Internet.

(e) If any component of the voting system is equipped with Wi-Fi capability or a wireless device, the county must ensure that the wireless capability or device is disabled before use in an election.

(f) The county may not connect any component of the voting system to another device by modem.

(g) The county may not alter, or grant permission to anyone else to alter, except during the trusted build process, the pre-boot settings for any voting system component, including altering the boot path.

(h) The county must include in its security plan the name, title and date of background checks for each employee with access to any of the areas or equipment set forth in this Rule. The county must maintain a storage facility access log that details employee name, date, and time of access to the storage facility in which the software, hardware, or components of any voting system are maintained. If access to the storage facility is controlled by use of key card or similar door access system that is capable of producing a printed paper log

including the person's name and date and time of entry, such a log must meet the requirements of this Rule. [Section 24-72-305.6, C.R.S.]

20.6.2 As of March 1, 2022, all users with access to the voting system must sign the voting system acceptable use policy agreement, provided by the Department of State, every year prior to using the system. The county must submit copies of all newly signed acceptable use policy agreements signed by election staff with the county's security plan.

20.6.3 A county may not create, permit any person to create, or disclose to any person an image of the hard drives of any voting system component without the express written approval by, and coordination with, the Department of State.

20.6.4 Removable storage devices

(a) The county must reformat all removable storage devices immediately before inserting them into any component of the voting system, except as provided in Rule 20.6.4(b) – (e), or in the conditions of use.

(b) The county may insert, without first reformatting, a removable storage device containing only election definition data files downloaded from SCORE if:

(1) The county reformats the removable storage device immediately before inserting it into the SCORE workstation and downloading the election definition data files; and

(2) Before and while downloading the SCORE election definition data, the county installs and operates the advanced network monitoring and threat detection applications provided or approved by the Department of State.

(c) The county may insert, without first reformatting, a removable storage device into a BMD, if:

(1) The removable storage device contains only election and ballot style data files necessary to program the BMD for testing or use in an election;

(2) The county downloaded the election and ballot style data files directly from the EMS workstation;

(3) The county did not expose the removable storage device to the internet or insert it into an internet-connected device after downloading the election and ballot style data files from the EMS; and

(4) The county reformatted the removable storage device immediately before inserting it into the EMS and downloading the election and ballot style data files.

(d) The county may insert a removable storage device without first reformatting it if the removable storage device contains only election database or project files remotely programmed by the voting system provider in accordance with Rule 20.8.

(e) The county may insert a removable storage device without first reformatting it if the removable storage device contains only election database backup files created by the county and:

(1) The county submits an attachment with their Security Plan stating security procedures for the removable storage device that addresses storage of the device when not in use; and

(2) The plan in the attachment is approved by the Department of State.

20.7 The county must keep all components of the voting system, ballots, servers, workstations, ballot scanners, BMDs, and video data records in a location with logs and access controls required by this Rule 20. The location must also be a temperature-controlled storage environment that maintains a minimum temperature of 50 degrees Fahrenheit and a maximum temperature of 90 degrees Fahrenheit. The storage environment must be dry with storage at least four inches above the floor. The county must provide the Department of State with a description of the specific environment used for each type of component.

20.8 Remote election programming services.

20.8.1 A county may not install or import into its voting system an election database or project programmed or created by the voting system provider using voting system components other than those owned or leased by the county and situated in the county's secure elections facility, unless the voting system provider first affirms on a form provided by the Secretary of State that:

(a) At all times during the election database or project programming, the voting system provider used only hardware and software certified for use in Colorado, as configured and verified during trusted build by the Secretary of State;

(b) At all times after installation of trusted build, the voting system provider operated all hardware utilized to program the election on a closed network, and did not connect the hardware to the internet or any internet-connected device;

(c) At all times during the election programming process, the voting system provider complied with the security protocols for removable storage devices in Rule 20.6.4(a) – (c); and

(d) The voting system provider physically delivered to the county removable storage media containing the finished election database or project, and did not transmit using any method connected or exposed to the internet.

20.9 Security cameras or other surveillance

20.9.1 The county must maintain a log of each person who enters the areas specified in Rule 20.9.3, including the person's name, signature, and date and time of entry. If access to the specified areas is controlled by use of key card or similar door access system that is capable of producing a printed paper log including the person's name and date and time of entry, the log must meet the requirements of this Rule.

20.9.2 Unless otherwise instructed, the county must make video security surveillance recordings of the areas specified in Rule 20.9.3 beginning at least 60 days before election day and continuing through at least 30 days after election day. If a recount or contest occurs, the recording must continue through the conclusion of all related activity. The recording system must ensure that records are not written over when the system is full. The recording system must provide a method to transfer the video records to a different recording device or to replace the recording media. If replaceable media is used then the county must provide a process that ensures that the media is replaced often enough to prevent periods when recording is not available.

20.9.3 The following are the specific minimum requirements:

(a) If the county has 50,000 or more registered voters, then the county must maintain a log and make video security surveillance recordings of the following areas, excluding voting booths:

(1) All areas in which election management software is used, including but not limited to programming, copying election files to memory cards or flash media, copying election files from memory cards or flash media, adjudicating ballots, tallying results, and results reporting.

(2) All areas used for processing ballots, including but not limited to areas used for Signature Verification, ballot opening, tabulation, or storage of voted ballots beginning at least 35 days before election day and continuing through at least 30 days after election day, unless there is a recount or contest. If a recount or contest occurs, the recording must continue through the conclusion of all related activity.

(3) The storage area for all voting equipment.

(b) If the county has fewer than 50,000 registered voters then the county must maintain a log and make video security surveillance recordings of all areas in which election management software is used, including but not limited to programming, copying election files to memory cards or flash media, copying election files from memory cards or flash media, tallying results, and results reporting.

(c) The county must adequately light the areas subject to video surveillance to provide visibility for video recording.

20.9.4 Video footage created under this rule must be maintained as an election record under section 1-7-802, C.R.S.

20.10 Equipment maintenance procedures. In addition to the requirements for voting systems inventory specified in Rule 11.2, the county must adhere to the following minimum standards:

20.10.1 The county must store all equipment throughout the year with seals over the data ports for each device. The county must maintain a log of the seals used for each device consistent to the logs used for tracking Election Day seals.

20.10.2 For equipment being sent to the vendor for offsite repairs/replacements, the county must keep a maintenance log for the device that must contain the following: the model number, serial number, and the type of device; the firmware version; the software version, as applicable; the printed name and signature of the person sending the equipment; the date of submission to the vendor; and the date the equipment is returned.

20.10.3 An employee must escort the vendor's representative at all times while on-site. At no time may the voting system vendor have access to any component of the voting system without supervision by an employee. [Section 24-72-305.6, C.R.S.]

20.10.4 Upon completion of any vendor maintenance, the county must verify or request reinstallation of the trusted build and conduct a full acceptance test of equipment that must, at a minimum, include the hardware diagnostics test, as indicated in Rule 11, and a mock election in accordance with this Rule. The county must maintain all documentation of the results of the acceptance testing on file with the specific device.

(a) If the maintenance was performed on a BMD, that BMD must be used to generate five ballots for use in the acceptance testing.

(b) If the maintenance was performed on a ballot scanner then at least five ballots (a combination of BMD-generated ballots and non-BMD-generated ballots – at least one of each) must be tabulated on the scanner.

20.10.5 A county must make available to the Department of State upon request, county documents and equipment, including:

(a) County maintenance records;

(b) Chain of custody logs;

(c) Trusted build integrity;

(d) Wireless status;

(e) Virus protection status;

(f) Password status (Bios, operating system, and applications);

(g) Access logs;

(h) Background check documents;

(i) Signed acceptable use policy agreements; and

(j) Video surveillance.

20.11 Transportation of equipment, ballot boxes, and ballots

20.11.1 The county must submit detailed plans to the Secretary of State before an election regarding the transportation of equipment and ballots both to remote voting sites and back to the central elections office or storage facility. If there is any evidence of possible tampering with a seal, or if the seal numbers do not match those listed in the chain-of-custody log, the county clerk must be immediately notified and must follow the procedures specific to the incident as described in Rule 20.15. While the method of transportation of equipment may vary, the following standards apply:

(a) Transportation by county personnel. County personnel must at all times display identification provided by the County. Two employee signatures and date are required at the departure location verifying that the equipment is sealed to detect tampering. Upon delivery of equipment, at least two election officials must verify, and indicate by signing and dating the chain-of-custody log, that all seals are intact and that the seal numbers match the logged seal numbers.

(b) Transportation by election judges. Election officials that are receiving equipment must inspect all voting devices and verify the specific seal numbers by signature and date on the chain-of-custody log for the device.

(c) Transportation by contract. If a county contracts for the delivery of equipment to remote voting locations, each individual delivering equipment must successfully pass a criminal background check. Any person who has been convicted of an election offense or an offense with an element of fraud is prohibited from

handling or delivering voting equipment. Two election officials must verify the specific seal numbers by device, sign, and date the chain-of-custody log upon release of the equipment to the individuals delivering the equipment.

20.11.2 Required procedures for transportation of ballot boxes:

(a) A bipartisan team, of election judges and/or staff, must seal all ballot boxes that contain voted ballots so that no person can access the ballots without breaking a seal. The team must record all seals in the chain-of-custody log, verify that the required seals are intact, and sign and date the log.

(b) A bipartisan team, of election judges and/or staff, must accompany all ballot boxes that contain voted ballots at all times, except when the ballot box is located in a vault or secure physical location.

(c) The ballot box exchange requirements of section 1-7-305, C.R.S., are met if a chain-in-custody log is completed for each ballot box.

(d) If a seal is broken or chain-of-custody is unverifiable, the county clerk must investigate, document his or her findings, and report the incident to the Secretary of State, as appropriate.

20.11.3 Ballot security at a voter service and polling center

(a) The county must secure unvoted paper ballots during pre-election storage, transportation, and at polling locations.

(1) Except when election judges are actively issuing ballots the ballot containers must be sealed and secure.

(2) The county must maintain chain-of-custody logs for all ballot containers,

(b) Unvoted paper ballots must be transported to polling locations in sealed containers. The county clerk must record the seal number on a chain-of-custody log for verification by the receiving election judges. The receiving election judges must verify the ballot container seal number before issuing ballots.

(c) When election judges are actively issuing ballots, the unvoted ballots must be in clear view of a minimum of two election judges of different party affiliations and one of the election judges must actively monitor the ballots unless the ballots are stored in a locked location accessible only to election officials.

(d) A minimum of two election judges of different party affiliations must reconcile and document all unvoted, issued, and spoiled paper ballots at the end of each day the polling center is open, and immediately report any inventory discrepancies to the county clerk.

(e) If unvoted paper ballots are stored overnight at the polling location, the ballots must be sealed in containers and stored in a locked location accessible only to election officials.

20.12 Contingency plans

20.12.1 The county must develop emergency contingency plans for voting equipment and voting locations in accordance with this Rule.

20.12.2 In the event of a serious or catastrophic equipment failure, or when equipment is removed from service, or there is not adequate backup equipment to meet the requirements of section 1-5-501, C.R.S., the county must notify the Secretary of State that the county is using provisional ballots as an emergency voting method.

20.12.3 The county contingency plans and evacuation procedures must address emergency situations including fire, severe weather, bomb threat, civil unrest, electrical blackout, equipment failure, and any other emergency situations the county identifies.

20.12.4 The county must develop procedures to address failures of SCORE continuity, which includes:

(a) Network failure,

(b) Power failure that lasts less than one hour, and

(c) Power failure that lasts more than one hour.

20.13 Anonymity.

20.13.1 Measures to protect anonymity include:

(a) The county may not keep any record indicating the order in which people voted on the BMD.

(b) When more than one BMD is available at a voting location, the county must, to the extent practicable, allow the voter to choose the BMD they wish to vote on.

20.13.2 The county clerk may not release a report generated from SCORE that includes a date and time stamp that could potentially identify a voter who cast a specific ballot.

20.13.3 The county must arrange voter service and polling center BMDs in a manner that prevents election officials and other voters from observing how a BMD voter marks or casts their ballot.

20.14 Security training for election officials. The county must include in its security plan the details of its security training. The county must address the anticipated time of training, location of training, and number of election officials receiving the security training, as it applies to the following requirements:

20.14.1 The county must conduct a separate training module for field technicians and election officials responsible for overseeing the transportation and use of the voting systems, picking up supplies, and troubleshooting device problems throughout the Election Day.

20.14.2 Security training must include the following components:

(a) Proper application and verification of seals and chain-of-custody logs;

(b) How to detect tampering with voting equipment, memory cards, or election data on the part of anyone coming in contact with voting equipment, including election officials, vendor personnel, or voters;

(c) Ensuring privacy in voting booths;

(d) Chain-of-custody requirements for voting equipment, activation cards, and other election materials;

(e) Ballot security;

(f) Voter anonymity; and

(g) Recognition and reporting of security incidents.

20.15 Remedies

20.15.1 If a seal is broken, or there is another discrepancy, the election official must immediately notify the county, who must remedy the discrepancy as follows:

(a) The county must verify the trusted build or the Secretary of State must reinstall trusted build. For instances where the county can display, verify, or print the hash value (MD5 or SHA-1) of the firmware or software, the election official must document and verify that the hash value matches the documented alphanumeric string associated with the trusted build for the software or firmware of that device.

(b) If the evidence indicates that the discrepancy occurred before the start of voting:

(1) The election officials must seal the device and securely deliver it to the county.

(2) The county must verify the trusted build or the Secretary of State must reinstall trusted build. Where the county can display, verify, or print the hash value (MD5 or SHA-1) of the firmware or software, the county must document and verify that the hash value matches the documented alphanumeric string associated with the trusted build for the software or firmware of that device.

(3) The county must reinstall the election programming into the device, conduct a hardware diagnostics test as prescribed in Rule 11, and conduct an acceptance test according to Rule 20.10.4, except that the device must be in full election mode, if applicable, and instead of casting or printing five ballots, the county must cast or print at least 25 ballots on the device. The county must maintain on file all documentation of testing and chain-of-custody for each specific device.

(4) The county must complete the necessary seal process and documentation to re-establish the chain-of-custody for the device and new memory card.

(5) The county must set the machine to election mode ready for a zero report.

(c) If the evidence indicates that the discrepancy occurred after votes were cast or printed on the device:

(1) The county may not continue to use the machine until verification or reinstallation of trusted build and acceptance testing is complete.

(2) The election officials must seal the device and securely deliver it to the county.

(3) The county must verify the trusted build or the Secretary of State must reinstall trusted build. Where the county can display, verify, or print the hash value (MD5 or SHA-1) of the firmware or software, the county must document and verify that the hash value matches the documented alphanumeric string associated with the trusted build for the software or firmware of that device.

(4) The county must complete the necessary seal process and documentation to establish the chain-of-custody for the device.

(5) The county must set the machine to election mode ready for a zero report before resuming voting on the device.

(6) Before certifying election results, the county must conduct a full (all contests) random audit on the device under Rule 25.3 and report results to the Secretary of State. This requirement is in addition to the post-election audit required by Rule 25.2 or 25.3.

20.15.2 The county must make all documentation related to the voting system and for every device used in the election available for Secretary of State inspection.

20.15.3 In the event that an election official knows, or reasonably should know, that the county's voting system was accessed by any individual not permitted access by these rules, or is made aware that the system has been tampered with, they must immediately notify the Department of State.

20.15.4 In the event that the Department of State determines that an election official has shown a serious or patterned failure to comply with any security requirements found in statute, these rules, the conditions of use of the voting system, or the acceptable use policy agreement for the voting system, the Department of State may take any or all of the following actions, including:

(a) Requiring the county to submit a security remediation plan no later than 90 days before the next election outlining the procedures the county will follow to ensure compliance with the security requirements that were not followed;

(b) Prohibiting or limiting the use of, as well as decertification of, a county's voting system or components in accordance with section 1-5-621, C.R.S., and Rule 21.7.3;

(c) In accordance with section 1-1.5-104 (2)(a)(II), C.R.S., appointing observers at the county expense to be present with the county to ensure compliance with the security requirements;

(d) Referring the matter to the Attorney General or District Attorney for potential investigation and prosecution under section 1-13-114, C.R.S. or any other applicable provision; or

(e) Taking any other action the Department of State deems necessary to ensure compliance.

20.16 A county may amend its security plan within 60 days of an election as a result of an unforeseen circumstance. The county must document the changes and file the revisions with the Secretary of State within five days of the change.

20.17 Lease, loan, or rental of election equipment. Nothing in this Rule requires a county to lease, loan, or rent any election equipment to any municipality, special district or other local jurisdiction.

20.17.1 A county that chooses to lease, loan, or rent any certified election equipment to a municipality, special district, or other local jurisdiction for use in their elections must maintain or reestablish an acceptable chain-of-custody and appropriate documentation in accordance with Rule 20.3.

20.17.2 Upon return of the voting equipment to the county, if the documentation and chain-of-custody does not support the proper maintenance of the trusted build software then the county must verify or request reinstallation of the trusted build before using the equipment.

20.17.3 To maintain the trusted build, the county must implement one of the following procedures:

(a) The county clerk must:

(1) Deliver the equipment to the jurisdiction;

(2) Witness and document the installation of the election programming used by the jurisdiction;

(3) Place one or more secure and numbered seals on the voting equipment in accordance with Rule 20.4. If during the course of the jurisdiction's election, the designated election official requires removal of a memory card or flash media as a function of the election process, the county clerk must witness and document the removal and proper resealing of the memory card or flash media; and

(4) Upon return of the equipment to the county, the county must verify, and indicate by signing and dating the chain-of-custody log, that all seals are intact. If any seal is damaged or removed, the county must verify or request the Secretary of State reinstate the trusted build; or

(b) The county must designate and station deputized county staff with the loaned equipment at all times while the equipment is under control of the designated election official. The deputized county staff must maintain physical custody of the equipment at all times to ensure that no unauthorized access occurs; or

(c) In accordance with section 1-5-605.5, C.R.S., the county must appoint the designated election official as a deputy for the purposes of supervising the voting equipment. The designated election official must:

(1) Sign and submit to the county an affirmation that he or she will ensure the security and integrity of the voting equipment at all times;

(2) Affirm that the use of the voting equipment is conducted in accordance with this Rule 20 the specific Conditions for Use of the voting equipment; and

(3) Agree to maintain all chain-of-custody logs for the voting devices.

20.18 Ballot on demand

20.18.1 The county must use the state-provided laptop for ballot on demand purposes only.

20.18.2 Software access, security, and storage.

(a) The county must change all Windows and ballot on demand application passwords at least once per calendar year.

(b) Only election officials or authorized vendor representatives may operate the ballot on demand system.

(c) The county may connect the ballot on demand laptop to an external network for the purpose of connecting to SCORE only if the county maintains current virus protection, current operating system security patches, and implements firewalls to prevent unauthorized access.

(d) The county must store the state-provided laptop and unused paper ballot stock in a locked storage area when the printer is not in use.

20.18.3 Ballot reconciliation

(a) The county must reconcile ballots printed on demand in accordance with Rules 10.1.1 and 10.1.2.

(b) The county must maintain damaged, misprinted, or unusable ballots as election records.

20.19 Voting system conditions for use

20.19.1 The county must use the voting system only on a closed network or in a standalone fashion.

20.19.2 Access logs.

(a) In addition to the audit logs generated by the election management system, the county must maintain access logs that record the following:

(1) The date, time, and user's name for each instance that a user enters or exits the system or the system's report printing functions; and

(2) Modifications to the system's hardware, including insertion or removal of removable storage media, or changes to hardware drivers.

(b) The county may create and maintain the access logs in the manner the county deems most suitable, including key stroke recording software, video surveillance recordings, manually or electronically written records, or a combination of these methods.

20.19.3 The county must create a backup copy of the election setup records on a read-only, write-once electronic storage media, immediately after completing the Logic and Accuracy Test.

(a) The county must identify the master database name and date of election on the label of the backup.

(b) The county must store the backup in a sealed container. Two election officials of different party affiliations must sign and date entries to the chain-of-custody log for the sealed container.

20.19.4 At least one BMD in each voter service and polling center must have a backup battery, or be connected to an uninterruptible power supply, sufficient to sustain continuous operation for a minimum of two hours in the event of power loss.

20.20 Trusted build procedures

20.20.1 When trusted build is required

(a) In the event that the Department of State determines a trusted build is required in a county, including due to a new certification, modification, or other security issue, the county and voting system provider must coordinate with the Department of State to install trusted build on a schedule determined by the Department of State.

(b) At the time that the Department of State determines a trusted build is required, the Department of State will provide the reason to the county for the required trusted build.

20.20.2 Attendance at trusted build

(a) The only individuals who may be present at a trusted build in a county include:

(1) Department of State staff, designees of the Department of State, or other individuals approved by the Department of State;

(2) Voting system vendor staff for the voting system for which trusted build is being installed; and

(3) The county clerk, employees of the county clerk, or the designated election official of the county, as long as those individuals are authorized to access the voting system under Rule 20.5.4 (a), have signed the voting system acceptable use policy agreement, and subject to the restrictions of Rule 20.5.3 (b).

(b) The county clerk and voting system vendor must provide the name, position, and proof of employment of individuals who will attend the trusted build in a county at the time of scheduling the trusted build with the Department of State.

(c) Background check

(1) Any individual present at the trusted build must have had a background check conducted in accordance with Rule 20.5.4 (a) – (c).

(2) The county clerk and voting system vendor must provide proof that a background check was conducted and passed on individuals who will be present to the Department of State at the time of scheduling the trusted build with the Department of State's office.

(d) The county clerk and voting system vendor may only allow the number of people designated by the Department of State for that county to attend the trusted build.

(e) If, due to an unforeseen circumstance, the county or voting system vendor must send an individual not previously identified to the trusted build, the county or vendor must immediately contact the Department of State and provide the

information otherwise required by this rule to the Department of State for the substitute individual.

20.20.3 Security at trusted build

(a) The county clerk must ensure that the location where the trusted build will be conducted does not allow for individuals who are not permitted to attend to be present or to otherwise disrupt the trusted build process.

(b) Video surveillance recording

(1) The county clerk must ensure that the trusted build is conducted under video surveillance as defined by Rule 1.1.44 until all devices are sealed at the conclusion of trusted build or acceptance testing.

(2) The county clerk must identify the video surveillance equipment that will be used to comply with this rule to those attending the trusted build.

(3) Video surveillance of the trusted build must be maintained as an election record under section 1-7-802, C.R.S.

(4) No one may surreptitiously record the trusted build by video or audio.

20.20.4 Completion of trusted build

(a) Counties must seal all voting system components in accordance with the most recent conditions of use issued by the Department of State for the county's voting system immediately upon conclusion of the trusted build unless the county proceeds to and completes acceptance testing on the same day that trusted build is completed.

(b) In the event that a county immediately proceeds to acceptance testing on the same day the trusted build is completed, a county must seal all voting system components in accordance with the most recent conditions of use issued by the Department of State for the county's voting system upon conclusion of the acceptance testing.

(c) The county must submit a copy of the signed trusted build affidavit to the Department of State following the completion of acceptance testing.

20.20.5 In the event that a trusted build cannot be scheduled or completed due to a county's violation of these rules or in the event that a county is found to have violated these rules following a trusted build, the Department of State may take any of the actions listed in Rule 20.15.4.